ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

STUDY AND ANALYSIS ON PACKET SNIFFING TOOL CAIN AND ABEL- A REVIEW

Urvashi Surjey*, Sonal Pansari, Yash Arya, Yash Katiyar, Neera Bansal

ABSTRACT

Packet sniffing is a process which uses software or hardware devices to monitor and capture all data packets that are passing through any given network. Packet sniffing is a kind of wiretap which overseer telephone or internet conversations. Using packet sniffers, network manager can triumph the confidential information of packets conveniently. After trapping the information, developer can access the networks or system easily. Sniffers, also called as network probes or snoops analyze creates a replicate of the data without modifying it.

INTRODUCTION

A Packet sniffer is software that monitors the data which is being conveyed over a network by the administrator. To govern both switched and non-switched environment, packet sniffing can be used. Sniffers are used both authorized functionality and for sneaking information from the network(without being intended). Unauthorized sniffers can be highly risky to network traffic's security. To deny the unauthorized access to the networks, security systems are applied but the unauthorized sniffers place the packet on network in promiscuous mode and in this mode the operation of encryption can be set on the network devices which grab private information that was secured by the authorized users and was not intended for the unauthorized users.

Packet sniffer is multipurpose that intended to itself and also to all hosts present on the network. On a local network, every machine will have their own MAC addresses which are different from other machines present on the network. When the transmission of packet occurs it will be present for all machines on local network. The NIC (Network Control Interface) of the machine on the network which is if kept in promiscuous mode can acquire all the packets and a frame.

The packet is accepted only if the MAC address of the machine matches the packet received by a NIC if not, it get filtered. The packet which is arrived at NIC end reproduce to device driver memory and then it is processed to kernek buffer end and is used by the user application.

The tool (Cain & Abel) works for Microsoft operating system. With the help of this tool, we can recover the password by sniffing the network. The tool will helps us to crack any encrypted password by using one of the methods like dictionary, brute force attack, cryptanalysis, uncovered caches password and it also help us to analyze the routing protocol. In the Cain and Abel tool, Cain is main analysis tool and with the help of Abel, we can take remote login on target machine, which can dump user hashes from the remote SAM even if it was encrypted using the "Syskey" utility and other features like the LSA Secrets dumper, the route table manager and the TCP/UDP Table Viewer. An appealing characteristic of Cain & Abel is APR (ARP Poison Routing) which enables sniffing on switched LANs by hijacking IP traffic of multiple hosts at the same time. The sniffer can also analyze encrypted protocols such as SSH-1 and HTTPS if used with APR and a Man-in-the-middle situation.

METHDOLOGY

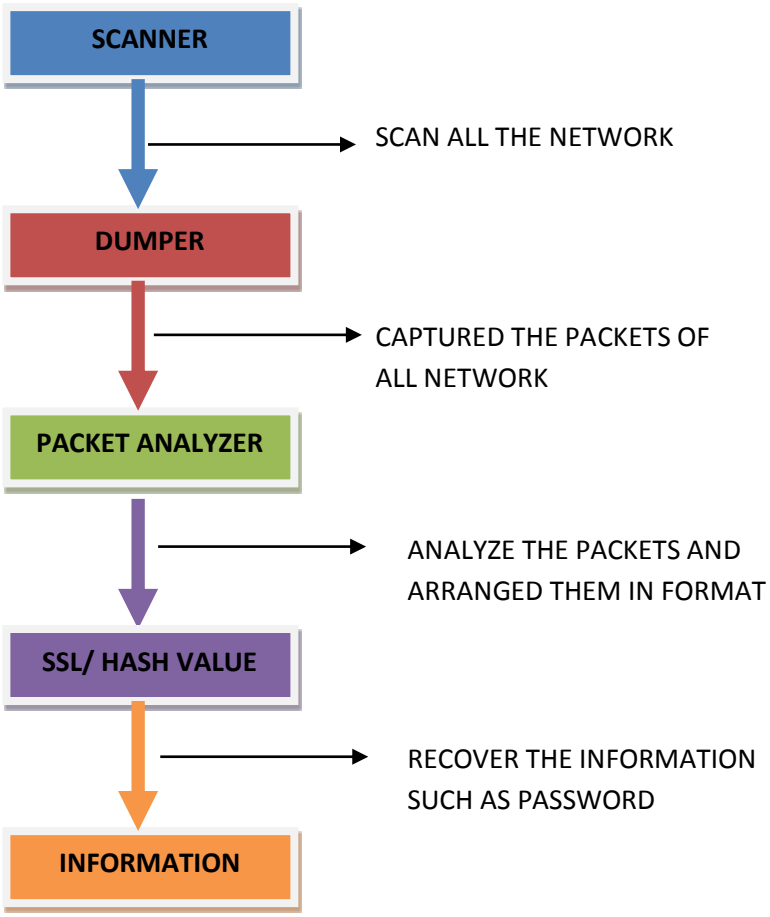

Figure 1: Process Flow Diagram

Step 1: Scanner
Scanner is a process that scans all the network systems and find out which network is accessible , also it traps the various application protocols(such as HTTP , HTTPS , Telnet ,FTP etc) running currently on a network .

Step 2: Dumper
Dumper is used to capture the packets transferred during the process over a network and list the protocol packets, which travel in all network which access by the user (HTTP, HTTPS, TELNET, all other network protocols).

Step 3: Packet Analyzer
The work of packet analyzer is to arrange the packets in a systematic manner so that the packets can be fetching in efficient manner for e.g. ethercap.

Step 4: SSL/Hash Value
If the data is encrypted i.e. if we have altered the meaning of the data via some means than with the help of SSL decoding techniques we can recover the data.
#the normal hash values, we can use some hexadecimal codes like MD5/ MD to recover the hash values. E.g. wincap and Tcpdump.

CONCLUSION

For security assessment process there are several tools available which are helpful for both customer and developer. In this summer internship I have explored one of the security tools which would be helpful to

conduct security assessment process. The Cain and Abel tool contains functionality like managing password, detecting vulnerability, malware detection, web page editor and password recovery.

REFERENCES

[1] C. Sanders, Practical Analysis Using Wireshark to Solve RealWorld Network Problems, 2nd ed., W. Pollock, USA, 2007.
[2] T. Dean, Network+ Guide to Networks, 6TH ed., D. Garza, S. Helba, Nelson Education, Canada, 2013.
[3] A. Orebaugh, Wireshark and Ethereal: Network Protocol Analyzer Toolkit, A. Williams, Canada, Syngress, 2007.
[4] K. Hassan, A. Ahsan, and M. Rahman, "IEEE 802.11b Packet Analysis to Imrove Network Performance", in JUJIT, 2012, Vol.1, p. 27-34.
[5] P. Asrodia, H. Patel, "Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis", in IJEECE, 2012, paper 2277-2626, p. 55-58
[6] D. Shinder (2005) Ethical-Issues-IT-Security-Professionals homepage on windowsecurity. [0nline]. Available: http://www.windowsecurity.com/articlestutorials /misc_network_security/Ethical-Issues-IT - Security- Professionals.html
[7] S. Venkatramulu, C. V. Rao, "Various Solutions for Address Resolution Protocol Spoofing Attack", in IJSRP, 2013, 2250-3153.
[8] S. Suri, V. Batra, "Comparative Study of Network Monitoring Tools", in IJITEE, 2012, paper 2278-3075, p. 63-65.
[9] J. Yerby, "Legal and Ethical issues of employee monitoring", in OJAKM, 2013, Vol. 1, Issue 2, p. 44-55.
[10] G. S. Alder, M. Schminke, T. W. Noel, and M. Kuenzi, "Emplyee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation", in JBE, 2008, paper 10.1007 , p. 481-498
[11] [online] http://www.wisegeek.org/how-do-employers-monitorinternet- usage-at- work.htm #didyouknowout
[12] S. Ansari, R. G. Rajeev, H. S. Chandrashekar, "Packet Sniffing: A Brief Introduction", in IEEE, 2003, paper 10.1109, p. 17 -19
[13] C. Gandhi, G. Suri, R. P. Golyan, P. Saxena, and B. K. Saxina, "Packet Sniffers- A Comparative Study", IJCNCS, paper 2308-9830, p. 179-187.
[14] R. Spangler, "Packet sniffer Detection with Antisniff", University of Wisconsin-Whitewater, department of Computer and Network Administration, 2003.
[15] [online]. Available: http://www.colasoft.com
[16] W. B. Pottner, L. Wolf, "IEEE 802.15.4 Packet Analysis with Wireshark and off-the-Shelf Hardware", in Proc. SICNSS, 2010.